PTO/SB/17 (12-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 12/8/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2005

☐ Applicant Claims small entity status. See 37 CFR 1.27

Complete if Known	
Application Number	09/911,592
Filing Date	July 24, 2001
First Named Inventor	Hoefelmeyer, et al.
Examiner Name	Chen, S.
Art Unit	2131
Customer No.	255373

TOTAL AMOUNT OF PAYMENT	($) 500.00	Attorney Docket No.	COS00019

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify):_____

☒ Deposit Account Deposit Account Number: 13-2491 Deposit Account Name: MCI, Inc.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)
☒ Charge fee(s) indicated below   ☐ Charges fee(s) indicated below, **except for the filing fee**

☐ Charge any additional fee(s) or underpayments of fee(s)   ☐ Credit any overpayments
under 37 CFR 1.16 and 1.17

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	Small Entity Fee ($)	SEARCH FEES Fee ($)	Small Entity Fee ($)	EXAMINATION FEES Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	_____
Design	200	100	100	50	130	65	_____
Plant	200	100	300	150	160	80	_____
Reissue	300	150	500	250	600	300	_____
Provisional	200	100	0	0	0	0	_____

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 or, for Reissues, each claim over 20 and more than in the original patent	50	25
Each independent claim over 3 or, for Reissues, each independent claim more than in the original patent	200	100
Multiple dependent claims	360	180

Total Claims	Extra Claims	Fee ($)	Fee Paid ($)
15 - 20 or HP =	0	x $50.00 =	$ 0.00

HP = highest number of total claims paid for, if greater than 20

Multiple Dependent Claims Fee ($)	Fee Paid ($)
$360.00	_____

Indep. Claims	Extra Claims	Fee ($)	Fee Paid ($)
5 - 5 or HP =	0	x $200.00 =	$ 0.00

HP = highest number of independent claims paid for, if greater than 3

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41 (a)(1)(G) and 37 CFR 1.16(s).

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof	Fee ($)	Fee Paid ($)
0 - 100 =	0	/ 50 = 0 (round up to a whole number) x	$250.00 =	$ 0.00

4. OTHER FEE(S)

	Fees Paid($)
Non-English Specification, $130 fee (no small entity discount)	_____
Other: Filing a brief in support of an appeal	$500.00

SUBMITTED BY

Signature	[signature]	Registration No. (Attorney/Agent)	44658	Telephone	(703) 425-8508
Name (Print/Type)	Phouphanomketh Ditthavong			Date	December 23, 2005
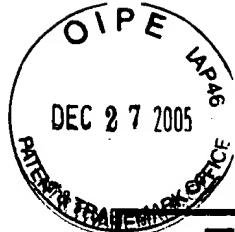
PTO/SB/21 (12-97)
Approved for use through 9/30/00. OMB 0651-0031
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paper Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
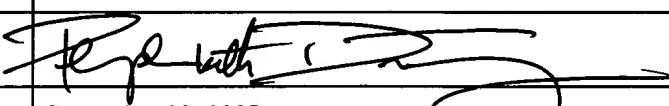
TRANSMITTAL FORM *(to be used for all correspondence after initial filing)*		
	Application Number	09/911,592
	Filing Date	July 24, 2001
	In re Application of:	Ralph Samuel HOEFELMEYER et al.
	Group Art Unit	2131
	Examiner Name	Chen, S.
	Customer No.	25537
Total Number of Pages in This Submission	31	Client Docket Number	COS00019

ENCLOSURES *(check all that apply)*
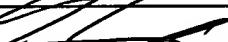
☒ Fee Transmittal Form	☐ Assignment Papers *(for an Application)*	☐ After Allowance Communication to Group
☐ Fee Attached	☐ Drawing(s)	☐ Appeal Communication to Board of Appeals and Interferences
☐ Amendment / Response	☐ Licensing-related Papers	☒ Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
☐ After Final	☐ Petition Routing Slip (PTO/SB/69) and Accompanying Petition	☐ Proprietary Information
☐ Affidavits/declaration(s)	☐ To Convert a Provisional Application	☐ Status Letter
☐ Extension of Time Request	☐ Power of Attorney, Revocation Change of Correspondence Address	☐ Additional Enclosure(s) *(please identify below):*
☐ Express Abandonment Request	☐ Terminal Disclaimer	
☐ Information Disclosure Statement	☐ Small Entity Statement	
☐ Certified Copy of Priority Document(s)	☐ Request of Refund	
☐ Response to Missing Parts/ Incomplete Application	Remarks	
☐ Response to Missing Parts under 37 CFR 1.52 or 1.53		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	DITTHAVONG & CARLSON, P.C. Phouphanomketh Ditthavong, Reg. No. 44658
Signature	
Date	December 23, 2005

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Alexandria, VA 22313-1450 on this date:

Type or printed name	Linda V. Wiley		
Signature		Date	December 23, 2005

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of: Ralph Samuel HOEFELMEYER et al.	Conf. No.: 3657
Application No.: 09/911,592	Group Art Unit: 2131
Filed: July 24, 2001	Examiner: Chen, S.
Customer No.: 25537 Attorney Docket: COS00019 Client Docket: 09710-1007	

For: NETWORK SECURITY ARCHITECTURE

APPEAL BRIEF

Honorable Commissioner for Patents
Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in support of the Notice of Appeal dated October 27, 2005.

I.   REAL PARTY IN INTEREST

MCI, Inc. is the real party in interest.

II.   RELATED APPEALS AND INTERFERENCES

Appellants are unaware of any related appeals and interferences.

III.   STATUS OF THE CLAIMS

Claims 1-15 are pending in this appeal. No claim is allowed. This appeal is therefore taken from the final rejection of claims 1-15 on July 26, 2005.

IV.   STATUS OF AMENDMENTS

No amendment to the claims has been filed since the final rejection of claims 1-15 on July 26, 2005.

V.   SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention relates to computer security and more particularly to a network security architecture. (*See, e.g.,* specification, ¶ 01)

With the explosion of global, computer communications spurred by the Internet, on-line organizations' need for protection against cyber-criminals and cyber-vandals has also been expanding. For example, data and network sabotage incidents continue to increase–by over 35% per year from 1997 to 1999. Financial fraud perpetrated on-line has increased 25% in the same period. Viruses, worms, Trojan horses and other malicious code continue to plague enterprise and home users, and many are global in scope, such as the infamous "love bug" worm of 2000. Warfare has even gone on-line, with cyber-terrorists in hot spots such as the Balkans and the Middle East making attacks on web sites and servers, and as the avowed tool of nation-states, notably the United States of America and the People's Republic of China. Mainstream press coverage of these events has heightened privacy and security concerns, hindering the widespread adoption of Internet commerce.

Accordingly, organizations need network security to protect organizations from malicious attacks over the Internet, whether by hackers or from viruses. In fact, the market for network

security is expanding rapidly, reaching a projected value of $10 billion by the end of the year 2001. Unfortunately, most network security approaches are ad-hoc and implemented on an organization-by-organization basis. These approaches not only tend to be staff-intensive and expensive, but they also quickly become out-of-date, falling behind the malicious technology that is constantly being developed by hackers. As a result, there is an urgent need for a scalable, network security architecture that can take advantage of economies of scale and simplify the provisioning of network security services to organizations. (*See, e.g.,* specification, ¶¶ 02-03)

The present invention addresses this and other needs by providing a scalable, layered, network, system and application security architecture that comprises a combination of server-based and client-based malicious code scanning components in conjunction with a firewall for diverting suspect traffic to decoy servers, and an overall security management system for attack correlation across the enterprise or network infrastructure. This security architecture can be deployed between the organization's intranet and internet backbone and can be shared between various organizations, thereby providing the economies of scale that conventional network security solutions lack. (*See, e.g.,* specification, ¶ 04)

Accordingly, one aspect of the present invention pertains to a network security system to be deployed between intranets that belong to subscribing organizations and an internet backbone. The server-based component is a scanning system that scans incoming electronic mail for malicious code. The client-based component is a malicious code detection FTP software server for downloading anti-virus code to clients on the intranets. A switch is provided for directing incoming electronic mail from the internet backbone to the scanning system so that the electronic mail can be scanned. (*See, e.g.,* specification, ¶ 05, claims 1, 3, 5, 8, 10) In addition to the switch, a Denial of Service (DoS) or Distributed DOS scanning/filtering switch may be employed

3

to prevent these specific attacks. In one embodiment, a decoy server is also provided for masquerading as a legitimate server and logging suspicious activity from communications received from the internet backbone. (*See, e.g.,* specification, ¶ 05, claims 2, 4, 7, 9,)

FIG. 1 is a block diagram of an exemplary network security architecture for combating viruses, malicious code, and other possible forms of attack from an outside user 101 via the Internet. This architecture employs a scalable, multi-layered approach that has both server-side and client-side components for antiviral defense, as well as the provision of firewalls for handling intruders. In one aspect, resilience is achieved by featuring multiple servers for redundancy. This architecture is also designed to be used by third parties under subscription, simply by turning on the third party's customer domain in the network. (*See, e.g.,* specification, ¶ 14)

In the architecture illustrated in FIG. 1, one or more front-end switches 110 are coupled to the Internet backbone 100 and provide the basic gate-keeping functionality of the architectures. In one implementation, the front-end switches 110 also measure and record the communications traffic between the customers' systems and the Internet for billing purposes. The front-end switches 110, which may be implemented with one or more CISCO™ 6509 switches, are thus responsible for receiving communications from the Internet backbone 110, directing the Internet communication to an appropriate security server for detecting and responding to incoming threats, and load balancing among the security servers. (*See, e.g.,* specification, ¶ 15, claims 1-11) Accordingly, the front-end switches 110 are positioned to intercept incoming electronic mail and other communications before they are routed to the customers' systems. The switches are also connected directly to DoS/DdoS scanning/filtering switches operating at line speed. (*See, e.g.,* specification, ¶ 15)

A local area network 120, such as a fast ETHERNET™ network, couples the front-end switches 110 with the security servers, which comprise, for example, one or more mail proxy servers 130, one or more antivirus scanning servers 140, one or more client antivirus servers 150, one or more decoy servers 160, and a quarantine server 170. The front-end switches 110, the mail proxy servers 130, the antivirus scanning servers 140, the client antivirus servers 150, and the decoy servers 160 are in communication with a hub 180, which communicates with client intranets 190 that belong to respective customers. (*See, e.g.,* specification, ¶ 16, claims 1-15)

One aspect of the present invention relates to a server-side antivirus deployment to protect client intranets 190 from incoming viruses and other kinds of malicious code. Referring to FIG. 2, incoming electronic mail is received by the front-end switches 110 from the Internet backbone 100 (step 201). This electronic mail may contain viruses that have been attached innocently or deliberately by the outside user 101, or may be embedded in the body of the e-mail itself, e.g., as an HTML bug or Java script. (*See, e.g.,* specification, ¶ 19)

At step 203, the front-end switches 110 direct the incoming electronic mail and any other messages received on the SMTP port over the local area network 120 to one of the mail proxy servers 130. (*See, e.g.,* specification, ¶ 20, claims 1, 3, 5, 8, 10) In addition to files, data streams or the actual body of a mail message or HTML page may contain scripts which may act maliciously. (*See, e.g.,* specification, ¶ 20)

The mail proxy server 130, in response at step 205, examines electronic mail messages to determine if the electronic mail messages and/or attachments need to be scanned for viruses. This determination can be done in accordance with a policy that may be set by the customer or the service provider, to permit setting a proper balance between security and performance. Accordingly, the particular policy may vary from implementation to implementation and, indeed,

from one installation to another. For example, the policy can state that all executable attachments should be scanned for viruses. The policy can also state that all documents with embedded macros should be scanned for viruses. In fact, one policy can specify that all electronic mail messages are to be scanned for viruses. When the mail proxy server 130 determines, in accordance with the policy, that the electronic mail message needs to be scanned, the mail proxy server 130 sends the electronic mail message to one or more of the antivirus scanning servers 140 for that operation (step 207). The mail proxy also verifies that either the sender or receiver of the message is an authorized user of this service. (*See, e.g.,* specification, ¶ 21, claims 1, 3, 5, 8, 10)

When the electronic mail message is received by one or more of the antivirus scanning servers 140, the electronic mail message is scanned for malicious code (step 209). In one implementation, antivirus scanning software on the one or more of the antivirus scanning servers 140 employs a catalog of viral signatures, which are often simple strings of bytes that are expected to be found in every instance of a particular virus. Usually, different viruses have different signatures, and the antivirus scanning software use signatures to locate specific viruses. To improve coverage, antivirus scanning software from multiple vendors may be employed, and the scanning may be performed on respective antivirus scanning servers 140 for improved performance. (*See, e.g.,* specification, ¶ 22)

If the electronic mail message is infected, tested at step 211, then the antivirus scanning server 140 may attempt to repair the infected portion of the electronic mail message, e.g. an attachment (step 213), as determined by policy. If the electronic mail message or its attachment cannot be repaired (tested at step 215), then the electronic mail message is quarantined (step 217) by transferring the original, infected electronic mail message to the quarantine server 170 and by removing the infected portion from the electronic mail message to create a sanitized electronic

mail message; this action may be varied by policy. The infected electronic mail message can be analyzed at the quarantine server 170 to study the virus, e.g. to generate a new viral signature or determine a new way to sanitize or repair a file infected with the virus. (*See, e.g.,* specification, ¶ 23, claims 12-15)

In either case, when the electronic mail message is infected, the sender and recipient of the electronic mail message may be notified of the detection of the viral infection (step 219), as determined by policy. This notification may be performed by appending text explaining the viral infection to the body of the electronic mail message or as a new attachment or even by composing and sending a new electronic mail message to the sender and recipient of the infected electronic mail message. (*See, e.g.,* specification, ¶ 24)

When the electronic mail message has been sanitized, by passing the antiviral scan (step 209), being repaired (step 213), or being quarantined (step 217), the sanitized electronic mail message is directed to the recipient, via hub 180 and the appropriate intranet 190. Accordingly, a scalable, resilient server-side antivirus scanning architecture is described, in which preferably multiple mail proxy servers 130 and antivirus scanning servers 140 are deployed to catch and sanitize incoming electronic mail messages. When malicious code is detected, an event is generated to the security management system. (*See, e.g.,* specification, ¶ 25, claims 12-15)

Another aspect pertains to distribution of client-side antivirus or other security software. Not all malicious code enters a company's computer network via incoming electronic mail messages or other kinds of files transferred from the Internet via a file transfer protocol. For example, malicious code may be transmitted to the company's computers or the company's intranet via files that are borne on portable computer-readable media, such as a floppy disk or CD-ROM, and inserted into one of the company's computers. As another example, the incoming

electronic mail message or transferred file is encrypted and cannot be scanned before the recipient decrypts the incoming file. *(See, e.g.,* specification, ¶ 26)

In accordance with this aspect, a system and method are provided for installing client-side antivirus scanning software on each of the company's computers. The client-side antivirus scanning software is responsible for scanning files that are borne on portable computer-readable medium or locally decrypted to determine whether the files are safe or need repair and/or quarantining. In conventional systems, it is difficult and staff-power intensive to maintain multiple installation of client-side antivirus scanning software, typically resulting in poor antivirus coverage because new updates to the client-side antivirus scanning software are not applied to the clients' systems. This difficulty is addressed in one aspect by providing a centralized client-side antivirus scanning software source and causing the client systems to automatically and periodically download updates. *(See, e.g.,* specification, ¶ 27, claims 1, 3, 5, 8, 10)

FIG. 3 illustrates the operation of one implementation of installing client-side antivirus scanning software. At step 301, an operator at one of the client's computers directs a browser to a location on one of the client antivirus servers 150, e.g. by typing the URL (Uniform Resource Locator) of a web page for downloading the client-side antivirus scanning software. In response, a web page is displayed at the client's browser and the operator performs an action (such as clicking on a button or pressing the return key) to initiate the installation.

At step 303, the installation request is received by the client antivirus server 150 from the browser. In response, the client antivirus server 150 checks the network address of the browser with a list of the subscribing clients' network addresses (step 305). If the network address of the browser does not match the list of subscribing clients' network addresses, then the request is

denied (step 315), thereby denying use of this system for non-subscribers. Alternatively, authorization to download the client-side antivirus scanning software can be controlled through passwords, public keys, or other forms of authentication, e.g., the profile management system.

If, on the other hand, the network address of the browser does indeed match the list of subscribing clients' network addresses, then execution proceeds to step 307 where the client antivirus server 150 opens a file transfer session to the client's computer. At step 309, the client-side antivirus scanning software is downloaded to the client's computer along with any data necessary, such as a database of updated viral signatures. The client-side antivirus scanning software is also configured at step 311, during this installation process, to periodically pull updates of the antivirus scanning software and data. To distribute the load for multiple clients' downloading the updates, a randomization function may be used to set a respective update time during an eight-hour window, e.g. between 10 p.m. and 6 a.m. Thus, the automatic updating of the client-side antivirus scanning software and data is evenly distributed throughout this period, rendering the system as a whole more scalable and resilient.

To ensure that the clients' computer systems will have the latest updates of the client-side antivirus scanning software, the client antivirus servers 150 are configured to periodically (e.g. by an entry in a UNIX™ cron table) to pull the latest updates from the vendors of the client-side antivirus scanning software (step 313). Accordingly, a scalable and extensible client-side antivirus scanning system is described, in which a common interface for installing the client-side antivirus scanning software is presented to each of the client's computers and configures the computers to automatically pull down the latest updates to the client-side antivirus scanning software and data on a periodic basis. As a result, the difficulties of conventional, staff-intensive approaches are alleviated. (*See, e.g.,* specification, ¶¶ 28-31, claims 1, 3, 5, 8, 10)

Computer viruses, whether communicated by electronic mail or through portable computer-readable media, are not the only security threats to a computer network. For example, a hacker could use active means, such as using a Telnet connection or the SubSeven Trojan horse, to intrude upon and possibly damage a computer system on the network. Accordingly, one aspect provides intrusion detection, such that intruders are diverted to a decoy environment in which the intruders' actions are monitored, controlled, and contained.

FIG. 4 is a flowchart illustrating the operation of one exemplary implementation for intrusion detection. At step 401, the front-end switches 110 received communications from an outside user 101 via the Internet backbone 100. These communications can take a variety of forms and may include, for example, telnet session, pings, and packets sent to any of the IP ports of computers in the intranets 190.

At step 403, the front-end switches 110 determine whether the communication source is authorized to transmit traffic into the intranets 190. Various approaches can be used to make this determination. For example, the front-end switches 110 may maintain a list of known, previously identified threat domains. In this example, all traffic originating from the identified threat domains are tagged as suspicious. In another example, traffic origination from any of suspect domains (also maintained in a list) is considered suspicious. In still another example, any traffic from specific unauthorized IP addresses are deemed suspicious. If the incoming communication uses ports that are not used by any of the applications on the customers' intranets 190, then the incoming communication is flagged as suspicious. If the incoming communication is authorized in the sense of not being determined to be suspicious (tested in step 405), then execution branches to step 415 where the authorized communication is routed to the destination within the intranets.

If, on the other hand, the incoming communication is not authorized (tested in step 405), then execution proceeds to step 407 where the incoming communication is routed to one of one or more decoy servers 160. A decoy server 160 is a computer system that is configured to look like the client's computer system. Thus, when the unauthorized communication is routed to the decoy server 160, the decoy server 160 simulates the client's computer system (step 409). Because the decoy server 160 is separate from the client's computer system, any activity at the decoy server 160 performed by the intruder will not affect the client's computer system. In one aspect, the decoy server 160 also includes some un-patched operating system/application holes to look more appealing or breakable to a would-be intruder.

When the intruder takes the bait of the decoy server 160, all actions and keystrokes of the intruder are logged to the administration console 161 (step 411). Consequently, the intruder's action can be studied to understand the nature of the intrusion and learn how to counter the intrusion or to ascertain the source of the intrusion. In addition, an electronic mail alert can be sent from the administration console 161 to an operator to inform that a penetration attempt is underway. (*See, e.g.*, specification, ¶¶ 32-36, claims 2, 4, 7, 9)

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 3, 5, 8, 10, and 12-15 are obvious under 35 U.S.C. § 103(a) based on *Hypponen et al.* (U.S. 2003/0191957) in view of *Hodges et al.* (U.S. 6,035,423).

Whether claims 2, 4, 7, and 9 are obvious under 35 U.S.C. § 103(a) based on *Hypponen et al.* and *Hodges et al.* further in view of *Almogy et al.* (U.S. 2002/0194489).

Whether claims 6 and 11 are obvious under 35 U.S.C. § 103(a) based on *Hypponen et al.* and *Hodges et al.* further in view of *Caccavale* (U.S. 2002/0129277).

VII.   ARGUMENT

A.   CLAIMS 1-15 ARE NOT RENDERED OBVIOUS OVER *HYPPONEN ET AL., HODGES ET AL., ALMOGY ET AL.,* AND *CACCAVALE.*

The initial burden of establishing a *prima facie* basis to deny patentability to a claimed invention under any statutory provision always rests upon the Examiner. *In re Mayne*, 104 F.3d 1339, 41 USPQ2d 1451 (Fed .Cir. 1997); *In re Deuel*, 51 F.3d 1552, 34 USPQ2d 1210 (Fed. Cir. 1995); *In re Bell*, 991 F.2d 781, 26 USPQ2d 1529 (Fed. Cir. 1993); *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In rejecting a claim under 35 U.S.C. § 103, the Examiner is required to provide a factual basis to support the obviousness conclusion. *In re Warner*, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967); *In re Lunsford*, 357 F.2d 385, 148 USPQ 721 (CCPA 1966); *In re Freed*, 425 F.2d 785, 165 USPQ 570 (CCPA 1970).

Obviousness rejections require some evidence in the prior art of a teaching, motivation, or suggestion to combine and modify the prior art references. See, e.g., *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1351-52, 60 USPQ2d 1001, 1008 (Fed. Cir. 2001); *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25, 56 USPQ2d 1456, 1459 (Fed. Cir. 2000); *In re Dembiczak*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

The Patent Office must give specific reasons why one of ordinary skill in the art would have been motivated to combine the references. See, e.g., *In re Kotzab*, 217 F.3d 1365, 1371, 55 USPQ2d 1313, 1317 (Fed. Cir. 2000); *In re Rouffet*, 149 F.3d 1350, 1359, 47 USPQ2d 1453, 1459 (Fed. Cir. 1998).

1.   **Claims 1, 3, 5, 8, 10, and 12-15 are not rendered obvious over** *Hypponen et al.* **in view of** *Hodges et al.*

a.   **Independent claims 1, 3, 5, 8, and 10 are not rendered obvious over** *Hypponen et al.* **in view of** *Hodges et al.*

Independent claim 1 recites (emphasis added):

1.   (Original) A network security system to be deployed between **a plurality of intranets belonging to respective organizations** and an internet backbone, comprising:

> a scanning system **coupled to the intranets** for scanning incoming electronic mail for malicious code;
> an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and
> a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:
>> directing incoming electronic mail from the internet backbone to the scanning system.

Thus, claim 1 recites a "scanning system **coupled to the intranets** for scanning incoming electronic mail for malicious code" in a "network security system to be deployed between a plurality of **intranets belonging to respective organizations** and an internet backbone." This feature is neither taught nor suggested in either *Hypponen et al.* or *Hodges et al.*

Hypponen et al. is directed to distributed computer virus detection and scanning (Title). Referring to FIG. 1 and the Abstract, *Hypponen et al.* describes a "method of detecting viruses in a computer network **1** comprising intercepting data at at least one data transit node **4** of the network **1**. The transit node **4** . . . transfers the identified data to a virus scanning server **7** over the network **1**." However, *Hypponen et al.* only shows one computer data network **1** in addition to the Internet **5** and has no disclosure of a "plurality of intranets," much less a "scanning system coupled to the intranets." Although the Examiner (Office Action dated July 26, 2005, p. 2, item 4) equates an "intranet" with the network **1** of *Hypponen et al.*, every feature of the claims,

including the plural "intranets," must be found in the applied references, and *Hypponen et al.*

lacks the recited plural "intranets."

In the "Response to Arguments" section, the Examiner (Office Action dated July 26,

2005, pp. 6-7, item 14) states:

> However, Hypponen discloses the transit node is coupled to a network and
> the transit node can be coupled to an external network or the transit node may be
> an internal node of the network (Hypponen: [0012]). On the other hand, the
> network can comprise a plurality of nodes and some of the nodes may be network
> server of another intranets [*sic*]. Therefore, one with ordinary skill in the art
> would apply the method disclosed by Hypponen in any environment.

Further, in the Advisory Action dated October 12, 2005, item 11, the Examiner states:

> Regarding applicant's remarks, applicant argues that the Hypponen reference does
> not disclose a scanning system coupled to the intranets and plurality of intranets
> belonging to respective organizations. However, Hypponen discloses the transit
> node is coupled to a network and the transit node can be coupled to an external
> network or the transit node may be an internal node of the network (Hypponen:
> [0012]). On the other hand, one with ordinary skill in the art would apply the
> method disclosed by Hypponen in any distributed environment.

The Examiner here focuses on paragraph [0012] of *Hypponen et al.*, which states:

> The transit node may be a gateway coupling the network to an external
> system or network, e.g. the Internet. Alternatively, the transit node may be an
> internal node of the network.

The next paragraph further clarifies the "transit node" (paragraph 13):

> Preferably, the transit node is one of a database server, an electronic mail
> server, an Internet server, a proxy server, and a firewall.

Nowhere does *Hypponen et al.* suggest that any node of the network 3 of Figure 1 is a

network server of "another intranet" as proposed by the Examiner, much less any nodes enabling

a "network security system to be deployed between a plurality of **intranets belonging to**

respective organizations and an internet backbone." Thus, the Examiner merely engages in a

wishful hindsight discussion of what the network "can comprise" and what some of the nodes

"can be." To establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). The Examiner has not met this burden.

Furthermore, this reasoning by the Examiner contravenes 35 U.S.C. § 132, which requires the Director to "notify the applicant thereof, stating the reasons for such rejection." This section is violated if the rejection "is so uninformative that it prevents the applicant from recognizing and seeking to counter the grounds for rejection." *Chester v. Miller*, 906 F.2d 1574, 15 USPQ2d 1333 (Fed. Cir. 1990). This policy is captured in the Manual of Patent Examining Procedure. For example, MPEP § 706 states that "[t]he goal of examination is to clearly articulate any rejection early in the prosecution process so that applicant has the opportunity to provide evidence of patentability and otherwise respond completely at the earliest opportunity." Furthermore, MPEP § 706.02(j) indicates that: "[i]t is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the applicant can be given fair opportunity to reply."

To the extent the Examiner relies on "common knowledge" in its assertions, Appellants respectfully submit that the Administrative Procedure Act (APA) requires the Patent Office to articulate and place on the record the "common knowledge" used to negate patentability. *In re Zurko*, No. 96-1285 (Fed. Cir., Aug. 2, 2001). *In re Lee*, 277 F.3d 1338, 1344-45, 61 USPQ2d 1430, 1434-35 (Fed. Cir. 2002). Ordinarily, there must be some form of evidence in the record to support an assertion of common knowledge. See *Lee*, 277 F.3d at 1344-45, 61 USPQ2d at 1434-35 (Fed. Cir. 2002); *Zurko*, 258 F.3d at 1386, 59 USPQ2d at 1697 (holding that general conclusions concerning what is "basic knowledge" or "common sense" to one of ordinary skill in

the art without specific factual findings and some concrete evidence in the record to support these findings will not support an obviousness rejection).

Hodges et al. too fails to disclose the plural "intranets" recited in the claims. Though the Examiner did not rely on *Hodges et al.* for this claim feature, it is evident from FIG. 10 of *Hodges et al.*, that there is only one corporate computer network **1006** on its side of the internet **1004**.

Independent claim 3 too is allowable over *Hypponen et al.* and *Hodges et al.* because neither reference shows "a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code." As for independent claim 5, neither *Hypponen et al.* nor *Hodges et al.* show a "plurality of scanning systems coupled to the intranets for scanning incoming electronic mail for malicious code."

Independent claims 8 and 10 recite: "downloading anti-virus code to clients coupled to the intranets." As discussed previously, neither *Hypponen et al.* nor *Hodges et al.*, nor any combination thereof, show plural intranets as required by the claims, and thus they do not render independent claims 8 and 10 obvious. Therefore, the rejection of independent claims 1, 3, 5, 8, and 10 is untenable and should be reversed.

> **b.   Dependent claims 12-15 are not rendered obvious over**
> ***Hypponen et al.* in view of *Hodges et al.***

Dependent claims 12-15 are allowable for at least the same reasons as their respective independent claims, and are separately patentable on their own merits. For example, dependent claim 12 recites, "**a hub** in communication with the scanning system **and the intranets**, wherein the scanning system is further configured for sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets and directing the sanitized incoming electronic mail

to the recipients via the hub." The Examiner (Office Action dated July 26, 2005, p. 4, item 7) contends that this feature is disclosed by *Hypponen et al.* at paragraphs [0037]-[0038]. However, the cited portion of *Hypponen et al.* merely discusses a single server 7 which provides virus scanning functionality (per paragraph [0034]) for the network 1 of *Hypponen et al.* If a virus is discovered by the virus scanning server 7, and the virus can be removed from the data by the server 7, then a disinfection operation is performed and the repaired data is returned to the originating system 4. There is no disclosure or suggestion of "**a hub** in communication with the scanning system **and the intranets**, wherein the scanning system is further configured for sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets and directing the sanitized incoming electronic mail to the recipients via the hub" as recited by claim 12. To establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). This burden has not been met by the Examiner. Therefore, the rejection of claims 12-15 should be reversed.

2. **Claims 2, 4, 7, and 9 are not rendered obvious over *Hypponen et al.* and *Hodges et al.* further in view of *Almogy et al.***

Dependent claims 2, 4, 7, and 9 are patentable for at least the same reasons as their independent claims and are individually patentable on their own merits. Further, the addition of *Almogy et al.* does not cure the deficiencies of *Hypponen et al.* and *Hodges et al.* as discussed previously with regard to independent claims 1, 3, 5, 8, and 10. For example, *Almogy et al.* does not disclose the "plurality of intranets belonging to respective organizations."

As another example, *Almogy et al.* does not disclose the "decoy server coupled to the intranets for masquerading as a legitimate server and logging activity on communications

received via the internet backbone" as recited in claims 2 and 4. In fact, *Almogy et al.* does not

even show a "decoy **server**" nor a server that masquerades as a legitimate server as recited in

claim 2, but what it calls "decoy addresses." Paragraph 153 (p. 7) of *Almogy et al.* states: "one or

more decoy addresses are inserted into either or both address book **102** and folders **104**." *Almogy*

et al.'s decoys are entities that are inserted into an address book; they are not servers.

In the "Response to Arguments" section, the Examiner (Office Action dated July 26,

2005, p. 7, item 15) states:

> However, Almogy discloses a virus detection and containment system
> which include at least one computer configured with at least one decoy address,
> and a server operative to identify activity occurring at the computer, the activity
> involving the decoy address (Almogy: [008]). The computers are being used as
> decoys to detect viruses.

Again, the Examiner engages in wishful claim construction, completely ignoring "decoy

server coupled to the intranets **for masquerading as a legitimate server** and logging activity on

communications received via the internet backbone" as recited in claims 2 and 4. A "server

operative to identify activity occurring at the computer," as urged by the Examiner, does not

obviate the features clearly recited by claims 2 and 4.

In the Advisory Action dated October 12, 2005, item 11, the Examiner states:

> Applicant further argues that the prior arts of record do not discloses [*sic*] decoy
> server. Applicant argues that the Almogy reference discloses "one or more decoy
> addresses are inserted into either or both address book 102 and folder 104."
> However, Almogy discloses a virus detection and containment system which
> include at least one computer configured with at least one decoy address (Almogy:
> [0008]). The computers are being used as decoys to detect viruses is known as the
> decoy server. Therefore, applicant's argument is respectfully traversed.

However, at paragraph [[0154], *Almogy et al.* states (emphasis added):

> In the method of FIG. 2, computer 100 becomes infected by a computer virus,
> such as by receiving the virus from another computer via a network 102 or via the
> introduction of infected data storage media such as a diskette or a compact disc
> into computer 100. As the virus attempts to propagate it selects one or more valid

and decoy addresses from address book 102 and folders 104, automatically generates messages that incorporate the virus, typically as an attachment, and forwards the messages to server 108. **Server 108 scans messages received from computer 100. Should server 108 detect a message addressed to a decoy address, server 108 may initiate one or more virus containment actions ...**

Thus, the server 108 of *Almogy et al.* is not "a **decoy server** coupled to the intranets for **masquerading as a legitimate server** and logging activity on communications received via the internet backbone" as recited at least by dependent claim 2, as the server 108 is a legitimate server that scans messages and detects messages addressed to a decoy address.

Dependent claim 7 recites "a plurality of decoy servers coupled to the intranets for masquerading as legitimate servers and logging activity on communications received via the internet backbone." Since *Almogy et al.* does not even disclose or suggest one such decoy server, it clearly does not show a plurality of such decoy servers.

Moreover, dependent claim 9 recites: "simulating the decoy server as a legitimate server to the suspicious traffic." *Almogy et al.*'s decoy addresses are not simulated as a legitimate server. To establish *prima facie* obviousness of a claimed invention, all of the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).

Therefore, the rejection of claims 2, 4, 7, and 9 should be reversed.

3.   **Claims 6 and 11 are not rendered obvious over *Hypponen et al.* and *Hodges et al.* further in view of *Caccavale.***

The addition of *Caccavale* does not cure the deficiencies of *Hypponen et al.*, *Hodges et al.*, and *Almogy et al.* as discussed previously with regard to independent claims 1, 3, 5, 8, and 10. Furthermore, dependent claims 6 and 11 are patentable for at least the same reasons as their independent claims and are individually patentable on their own merits. For example, dependent

claim 6 recites, "the switches are further configured for: load-balancing among the scanning

systems and among the decoy servers." Dependent claim 11 recites, "load-balancing among the

mail proxy servers." The Examiner (Office Action dated July 26, 2005, p. 6, item 12) states:

> Hypponen as modified does not explicitly disclose wherein the switches are
> further configured for: load-balancing among the scanning systems and among the
> decoy servers. However, Caccavale discloses perform load-balancing procedure
> when there are plurality of virus checking programs (Caccavale: [0012]). It would
> have been obvious to one having ordinary skill in the art at the time of applicant's
> invention to combine the teachings of Caccavale within the combination of
> Hypponen-Hodges because load-balancing is well known in the art to prevent
> denial of service attack and it increases efficiency of the process.

Appellants respectfully submit that *Caccavale*, at paragraph [0012] states (emphasis

added):

> [0012] In accordance with another aspect, the invention provides a method of
> operating a network file server to initiate a **virus scan upon a file stored in the
> network file server**. The network file server is coupled to at least one client for
> access of the client to at least one file in the network file server, and the network
> file server is coupled to a plurality of secondary servers for access of the secondary
> servers to the file stored in the network file server. The network file server
> includes a cached disk array and a plurality of data mover computers coupled to
> the data network and coupled to the cached disk array **for responding to client
> requests for data access to storage in the cached disk array**. Each secondary
> server is programmed with **a virus checker program executable for performing
> an anti-virus scan upon file data in random access memory of the secondary
> server**. The method includes at least one of the data movers in the network file
> server responding to a request for access from the client to the file in the network
> file server by **applying a filter upon a file extension of the file** upon opening or
> closing of the file to determine that an anti-virus scan of the file should be
> performed, and **initiating the anti-virus scan of the file by applying a load
> balancing procedure for selecting one of the secondary servers for
> performing the anti-virus scan of the file, and sending to the selected
> secondary server a request for the anti-virus scan including a specification of
> the file**. Then the selected secondary server responds to the request for the anti-
> virus scan by invoking the virus checker program in the selected secondary server
> to perform an anti-virus scan of the specified file by obtaining file data of the file
> from the network file server and storing the file data of the file into the random
> access memory of the selected secondary server and performing the anti-virus scan
> upon the file data of the file in the random access memory of the selected
> secondary server.

Thus, the "load balancing" mentioned by *Caccavale* has nothing to do with preventing a "denial of service attack" as urged by the Examiner in the supposed motivation to combine the references. Obviousness rejections require some evidence in the prior art of a teaching, motivation, or suggestion to combine and modify the prior art references. See, e.g., *McGinley v. Franklin Sports, Inc.*, 262 F.3d 1339, 1351-52, 60 USPQ2d 1001, 1008 (Fed. Cir. 2001); *Brown & Williamson Tobacco Corp. v. Philip Morris Inc.*, 229 F.3d 1120, 1124-25, 56 USPQ2d 1456, 1459 (Fed. Cir. 2000); *In re Dembiczak*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999).

Further, the "load balancing" mentioned by *Caccavale* has nothing to do with any type of load balancing among "mail proxy servers," nor among "a plurality of scanning systems coupled to the intranets for scanning incoming electronic mail for malicious code" as recited by the claims. Thus, *Caccavale* is not analogous prior art. "In order to rely on a reference as a basis for rejection of an applicant's invention, the reference must either be in the field of the applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." *In re Oetiker*, 977 F.2d 1443 (Fed. Cir. 1992); see also *In re Clay*, 966 F.2d 656 (Fed. Cir. 1992) ("A reference is reasonably pertinent if, even though it may be in a different field from that of the inventor's endeavor, it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering his problem.").

Moreover, it is well settled that the problem addressed and solved by a claimed invention must be given consideration in resolving the ultimate legal conclusion of obviousness under 35 U.S.C. § 103. *North American Vaccine, Inc. v. American Cyanamid Co.*, 7 F.3d 1571, 28 USPQ 1333 (Fed. Cir. 1993); *In re Dillon*, 919 F.2d 688, 16 USPQ2d 1897 (Fed. Cir. 1990); *Northern*

Telecom, Inc. v. Datapoint Corp., 908 F.2d 931, 15 USPQ 1321 (Fed. Cir. 1990); *Jones v. Hardy*, 727 F.2d 1524, 220 USPQ 1021 (Fed. Cir. 1984).

Unless the patent otherwise provides, a claim term cannot be given a different meaning in the various claims of the same patent. *Georgia Pacific Corp. v. U.S. Gypsum Co.*, 195 F.3d 1322, 1331, 52 USPQ2d 1590, 1598 (Fed. Cir., Nov. 1, 1999); see also *Southwall Tech., Inc. v. Cardinal IG Co.*, 54 F.3d 1570, 1579, 34 USPQ2d 1673, 1679 (Fed. Cir. 1995) (holding that claim term found in different claims must be interpreted consistently); *Fonar Corp. v. Johnson & Johnson*, 821 F.2d 627, 632, 3 USPQ2d 1109, 1113 (Fed. Cir. 1987.) (holding that a term used in one claim had the same meaning in another claim).

Well-settled case law holds that the words of a claim must be read as they would be interpreted by those of ordinary skill in the art. *In re Baker Hughes Inc.*, 215 F.3d 1297, 55 USPQ2d 1149 (Fed. Cir. 2000); *In re Morris*, 127 F.3d 1048, 1054, 44 USPQ2d 1023, 1027 (Fed. Cir. 1997); M.P.E.P. 2111.01. "Although the PTO must give claims their broadest reasonable interpretation, this interpretation must be consistent with the one that those skilled in the art would reach." *In re Cortright*, 165 F.3d 1353, 1369, 49 USPQ2d 1464, 1465 (Fed. Cir. 1999).

Since *Caccavale* is non-analogous art, *Caccavale* teaches away from combining the reference with *Hypponen et al.* and *Hodges et al.* It is improper to combine references where the references teach away from their combination. *In re Grasselli*, 713 F.2d 731, 218 USPQ 769 (Fed. Cir. 1983). A prior art reference must be considered in this entirety including portions that would lead away from the claimed invention. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984).

If a proposed modification would render the prior art being modified unsatisfactory for its

intended purpose, then there is no suggestion or motivation to make the proposed modification.

In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

If the proposed modification or combination of the prior art would change the principle of

operation of the prior art invention being modified, then the teachings of the references are not

sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349

(CCPA 1959). MPEP § 2143.01

Thus, the rejection of dependent claims 6 and 11 should be reversed.

## VIII. <u>CONCLUSION AND PRAYER FOR RELIEF</u>

For the foregoing reasons, Appellants request the Honorable Board to reverse each of the

Examiner's rejections.

Respectfully Submitted,

DITTHAVONG & CARLSON, P.C.

12/23/05
_____
Date
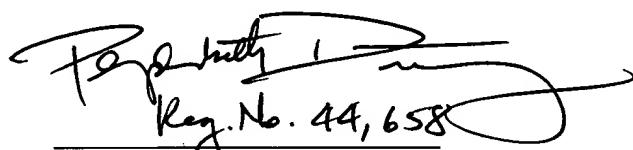
_____
Reg. No. 44,658
Margo Livesay
Attorney for Applicant(s)
Reg. No. 41,946

10507 Braddock Rd, Suite A
Fairfax, VA 22032
Tel. 703-425-8501
Fax. 703-425-8518

IX.   <u>CLAIMS APPENDIX</u>

1. (Original)   A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code;

an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and

a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:

directing incoming electronic mail from the internet backbone to the scanning system.

2. (Original)   A network security system according to claim 1, further comprising:

a decoy server coupled to the intranets for masquerading as a legitimate server and logging activity on communications received via the internet backbone;

wherein the switch is further coupled to the decoy server and is further configured for redirecting suspicious traffic from the internet backbone to the decoy server.

3. (Previously Presented)   A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a scanning system coupled to the intranets for scanning incoming electronic mail for malicious code;

a mail proxy server for determining whether the incoming electronic mail is to be scanned for malicious code and directing the incoming electronic mail to the scanning system when the incoming electronic mail is determined to be scanned for malicious code;

an anti-virus server coupled to the intranets for downloading anti-virus code to clients coupled to the intranets; and

a switch coupled between the internet backbone, the scanning system, and the anti-virus server, said switch configured for:

directing incoming electronic mail from the internet backbone to the mail proxy server.

4. (Previously Presented)   A network security system according to claim 3, further comprising:

a decoy server coupled to the intranets for masquerading as a legitimate server and logging activity on communications received via the internet backbone;

wherein the switch is further coupled to the decoy server and is further configured for redirecting suspicious traffic from the internet backbone to the decoy server.

5. (Original)   A network security system to be deployed between a plurality of intranets belonging to respective organizations and an internet backbone, comprising:

a plurality of scanning systems coupled to the intranets for scanning incoming electronic mail for malicious code;

a plurality of anti-virus servers coupled to the intranets for downloading anti-virus code to clients coupled to the intranets;

a plurality of switches coupled between the internet backbone, the scanning systems, and the anti-virus servers, said switches configured for:

directing incoming electronic mail to at least one of the scanning systems.

6. (Original)   A network security system according to claim 5, wherein the switches are further configured for:

load-balancing among the scanning systems and among the decoy servers.

7. (Original) A network security system according to claim 5, further comprising:

a plurality of decoy servers coupled to the intranets for masquerading as legitimate servers

and logging activity on communications received via the internet backbone;

wherein the switches are further coupled to the decoy servers and are further configured for

redirecting suspicious traffic from the internet backbone to the decoy servers.

8. (Original) A method for maintaining network security system between a plurality of

intranets belonging to respective organizations and an internet backbone, comprising:

directing incoming electronic mail from the internet backbone to a scanning system;

scanning incoming electronic mail for malicious code; and

downloading anti-virus code to clients coupled to the intranets.

9. (Original) A method according to claim 8, further comprising:

redirecting suspicious traffic from the internet backbone to the decoy server;

simulating the decoy server as a legitimate server to the suspicious traffic; and

logging activity on communications received via the internet backbone.

10. (Original) A method for maintaining network security system between a plurality of

intranets belonging to respective organizations and an internet backbone, comprising:

directing incoming electronic mail from the internet backbone to one of a plurality of mail

proxy servers;

at the one of the mail proxy servers, determining whether the incoming electronic mail is to

be scanned for malicious code and directing the incoming electronic mail to a scanning

system when the incoming electronic mail is determined to be scanned for malicious

code;

at the scanning system, scanning incoming electronic mail for malicious code;

downloading anti-virus code to clients coupled to the intranets.

11. (Original) A method according to claim 10, further comprising:

load-balancing among the mail proxy servers.

12. (Previously Presented) A network security system according to claim 1, further

comprising:

a hub in communication with the scanning system and the intranets, wherein the scanning

system is further configured for sanitizing at least some of the incoming electronic mail

addressed to recipients on the intranets and directing the sanitized incoming electronic

mail to the recipients via the hub.

13. (Previously Presented) A network security system according to claim 3, further

comprising:

a hub in communication with the scanning system and the intranets, wherein the scanning

system is further configured for sanitizing at least some of the incoming electronic mail

addressed to recipients on the intranets and directing the sanitized incoming electronic

mail to the recipients via the hub.

14. (Previously Presented) A method according to claim 8, further comprising:

sanitizing at least some of the incoming electronic mail addressed to recipients on the

intranets; and

directing the sanitized incoming electronic mail to the recipients on the intranets.

15. (Previously Presented) A method according to claim 10, further comprising performing, at the scanning system, the steps of:

sanitizing at least some of the incoming electronic mail addressed to recipients on the intranets; and

directing the sanitized incoming electronic mail to the recipients on the intranets via a hub in communication with the scanning system and the intranets.

X.   <u>EVIDENCE APPENDIX</u>

Appellants are unaware of any evidence that is required to be submitted in the present Evidence Appendix.

XI.   <u>RELATED PROCEEDINGS APPENDIX</u>

Appellants are unaware of any related proceedings that are required to be submitted in the present Related Proceedings Appendix.